

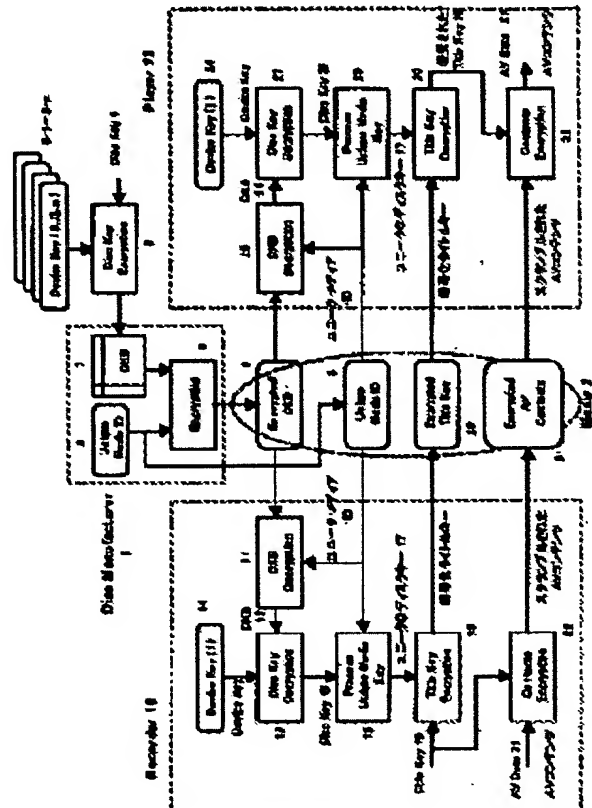
# INFORMATION RECORDING MEDIUM, RECORDER, RECORDING METHOD, REPRODUCING DEVICE, REPRODUCING METHOD, RECORDING AND REPRODUCING METHOD AND TRANSMITTING METHOD

**Publication number:** JP2001216727  
**Publication date:** 2001-08-10  
**Inventor:** YOKOUCHI KENTARO  
**Applicant:** VICTOR COMPANY OF JAPAN  
**Classification:**  
 - International: **G11B20/10; G11B20/10; (IPC1-7): G11B20/10**  
 - European:  
**Application number:** JP20000022128 20000131  
**Priority number(s):** JP20000022128 20000131

Report a data error here

## Abstract of JP2001216727

**PROBLEM TO BE SOLVED:** To unnecessitate special medium structure, to make reproduction impossible when contents recorded on a recording medium is copied wholly and to normally reproduce a medium recorded by normal recording. **SOLUTION:** Key information in a recording medium is enciphered double and recorded in a recording medium having a characteristic ID different by each medium.



Data supplied from the [esp@cenet](mailto:esp@cenet) database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2001-216727  
(P2001-216727A)

(43) 公開日 平成13年8月10日 (2001.8.10)

(51) Int.Cl.<sup>7</sup>

G 1 1 B 20/10

識別記号

F I

C 1 1 B 20/10

テーマト\* (参考)

H 5 D 0 4 4

審査請求 未請求 請求項の数11 O L (全 18 頁)

(21) 出願番号 特願2000-22128(P2000-22128)

(22) 出願日 平成12年1月31日 (2000.1.31)

(71) 出願人 000004329

日本ビクター株式会社

神奈川県横浜市神奈川区守屋町3丁目12番地

(72) 発明者 横内 健太郎

神奈川県横浜市神奈川区守屋町3丁目12番地  
日本ビクター株式会社内

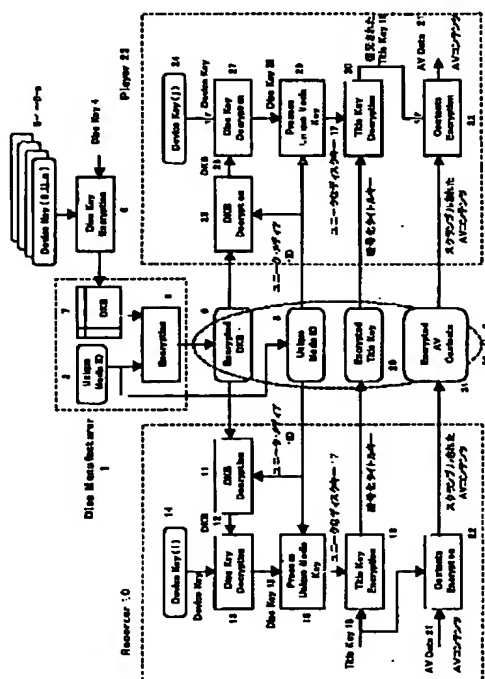
Fターム(参考) 5D044 B002 C004 DE50 DE57 EF05  
FG18 GK17 HL08

(54) 【発明の名称】 情報記録媒体、記録装置、記録方法、再生装置、再生方法、記録再生方法および伝送方法

(57) 【要約】

【課題】 特殊な媒体構造が不要で、記録媒体上に記録されたコンテンツが丸ごとコピーされた場合は再生を不可能とし、正規の記録で記録された媒体は正常に再生が可能とする。

【解決手段】 一枚毎に異なる固有のIDを有する記録媒体に記録媒体のキー情報を二重に暗号化して記録する。



【特許請求の範囲】

【請求項1】媒体固有データが記録された書き換え不可能な非データ領域である第1の領域と、

第1のキーデータを第2のキーデータで暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが記録されている第2の領域と、

ユーザデータの記録領域である書き換え可能な第3の領域とを有することを特徴とする情報記録媒体。

【請求項2】媒体固有データが記録された書き換え不可能な非データ領域と、

第1のキーデータを第2のキーデータで暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータ、およびユーザデータが記録される書き換え可能な領域とを有することを特徴とする情報記録媒体。

【請求項3】請求項1あるいは請求項2に記載の情報記録媒体において、前記媒体固有データはユニーク・メディア・IDで、前記第1のキーデータは単一のディスクキーで、前記第2のキーデータは複数のデバイスキーで、前記第1の暗号化キーデータは前記ディスクキーを前記複数のデバイスキーで暗号化した暗号化ディスクキーブロックで、前記第2の暗号化キーデータは前記暗号化ディスクキーブロックを前記ユニーク・メディア・IDで暗号化したユニークメディア暗号化ディスクキーブロックであることを特徴とする情報記録媒体。

【請求項4】データの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録する記録装置であって、

前記第1の暗号化キーデータから前記第1のキーデータを復号するために予め割り当てられた前記第2のキーデータ群のうちのいずれかの復号鍵を記憶する記憶手段と、

前記情報記録媒体から前記媒体固有データを読み出す手段と、

前記情報記録媒体から前記第2の暗号化キーデータを読み出す手段と、

前記読み出した媒体固有データおよび前記読み出した第2の暗号化キーデータを用いて前記第1の暗号化キーデータを復号する第1の復号手段と、

前記復号鍵および前記復号された第1の暗号化キーデータを用いて前記第1のキーデータを復号する第2の復号手段と、

前記復号された第1のキーデータおよび前記読み出された媒体固有データから中間鍵データを生成する手段と、

記録時にユーザーが決める前記コンテンツ毎に異なる第3のキーデータを前記中間鍵データで暗号化する第1の暗号手段と、

記録する前記コンテンツを前記第3のキーデータで暗号化する第2の暗号手段と、

前記第1の暗号化手段で暗号化された前記第3のキーデータおよび前記第2の暗号化手段で暗号化された前記コンテンツを前記情報記録媒体の前記書き換え可能な領域に記録する記録手段とを有することを特徴とする記録装置。

【請求項5】データの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録する記録方法であって、

前記記録媒体から前記媒体固有データを読み出し、前記記録媒体から前記第2の暗号化キーデータを読み出し、

前記読み出した媒体固有データおよび前記読み出した第2の暗号化キーデータを用いて前記第1の暗号化キーデータを復号し、

前記第1の暗号化キーデータを復号するために予め割り当てられた前記第2のキーデータ群のうちのいずれかの復号鍵で前記第1の暗号化キーデータを復号して前記第1のキーデータを復号し、

前記復号された前記第1のキーデータおよび前記媒体固有データから中間鍵データを生成し、

記録時にユーザーが決める前記コンテンツ毎に異なる第3のキーデータを前記中間鍵データで第3の暗号化キーデータを生成し、

記録する前記コンテンツを前記第3の暗号化キーデータで暗号化して暗号化コンテンツを生成し、

前記第3の暗号化キーデータおよび前記暗号化コンテンツを前記情報記録媒体の前記書き換え可能な領域に記録することを特徴とする記録方法。

【請求項6】データの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体であって、

コンテンツの記録時に、前記第2の暗号化キーデータを前記媒体固有データで復号した前記第1の暗号化キーデータを、さらに予め割り当てられた前記第2のキーデータ群のうちのいずれかの復号鍵で復号した前記第1のキーデータおよび前記媒体固有データを用いて生成した中

間鍵データで記録時にユーザーが決めるコンテンツ毎に異なる第3のキーデータを暗号化した第3の暗号化キーデータと、

前記第3のキーデータを鍵として前記コンテンツを暗号化した暗号化コンテンツとが前記書き換え可能な領域に記録されていることを特徴とする情報記録媒体。

【請求項7】データの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録するにあたり、

前記第2の暗号化キーデータを前記媒体固有データで復号した前記第1の暗号化キーデータを予め割り当てられた前記第2のキーデータ群のうちのいずれかの第1の復号鍵で復号された前記第1のキーデータおよび前記媒体固有データを用いて生成した中間鍵データで、記録時にユーザーが決めるコンテンツ毎に異なる第3のキーデータを暗号化した第3の暗号化キーデータと、

前記第3のキーデータを鍵として前記コンテンツを暗号化した暗号化コンテンツとが前記書き換え可能な領域に記録されている情報記録媒体より前記コンテンツを再生する再生装置であって、

前記第1の暗号化キーデータから前記第1のキーデータを復号するために予め割り当てられた前記第2のキーデータ群のうちのいずれかの第2の復号鍵を記憶する記憶手段と、

前記情報記録媒体から前記媒体固有データを読み出す手段と、

前記情報記録媒体から前記第2の暗号化キーデータを読み出す手段と、

前記読み出した媒体固有データおよび前記読み出した第2の暗号化キーデータを用いて前記第1の暗号化キーデータを復号する第1の復号手段と、

前記第2の復号鍵および前記復号した第1の暗号化キーデータを用いて前記第1のキーデータを復号する第2の復号手段と、

前記復号した第1のキーデータおよび前記読み出した媒体固有データから前記中間鍵データを生成する手段と、前記書き換え可能な領域から前記第3の暗号化キーデータを読み出し、前記読み出した第3の暗号化キーデータおよび前記中間鍵データを用いて前記第3のキーデータを復号する第3の復号手段と、

前記書き換え可能な領域から前記暗号化コンテンツを読み出し、前記第3の復号化手段で復号された前記第3のキーデータおよび前記暗号化コンテンツを用いて前記コンテンツを復号する第4の復号手段とからなることを特徴とする再生装置。

【請求項8】データの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録するにあたり、

前記第2の暗号化キーデータを前記媒体固有データで復号した前記第1の暗号化キーデータを前記第2のキーデータ群のうちのいずれかの第1の復号鍵で復号された前記第1のキーデータおよび前記媒体固有データを用いて生成した中間鍵データで、記録時にユーザーが決めるコンテンツ毎に異なる第3のキーデータを暗号化した第3の暗号化キーデータと、

前記第3のキーデータを鍵として前記コンテンツを暗号化した暗号化コンテンツとが前記書き換え可能な領域に記録されている情報記録媒体より前記コンテンツを再生する再生方法であって、

前記情報記録媒体から前記媒体固有データを読み出し、前記情報記録媒体から前記第2の暗号化キーデータを読み出し、

前記読み出した媒体固有データおよび前記読み出した第2の暗号化キーデータから前記第1の暗号化キーデータを復号し、

前記第1の暗号化キーデータ復号するために予め割り当てられた前記第2のキーデータ群のうちのいずれかの第2の復号鍵および前記第1の暗号化キーデータを用いて前記第1のキーデータを復号し、

前記復号した第1のキーデータおよび前記読み出した媒体固有データから前記中間鍵データを生成し、

前記中間鍵データおよび前記第3の暗号化キーデータを用いて前記第3のキーデータを復号し、

前記書き換え可能な領域から前記暗号化コンテンツを読み出し、前記復号した前記第3のキーデータおよび前記暗号化コンテンツを用いて前記コンテンツを復号することを特徴とする再生方法。

【請求項9】データの書き換え不可能な領域と、データの書き換え可能な領域とを有し、前記書き換え不可能な領域には媒体固有データが記録され、前記書き換え可能な領域には第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを前記媒体固有データで暗号化した第2の暗号化キーデータが予め記録された情報記録媒体を用いた記録再生方法であって、記録する際には、前記記録媒体より前記媒体固有データを読み出し、

前記記録媒体から前記第2の暗号化キーデータを読み出し、

前記読み出した媒体固有データおよび前記読み出した第2の暗号化キーデータを用いて前記第1の暗号化キーデ

ータを復号し、  
 前記第1の暗号化キーデータを復号するために予め割り当てられている前記第2のキーデータ群のいずれかの復号鍵および前記復号された第1の暗号化キーデータを用いて前記第1のキーデータを復号し、  
 前記復号された前記第1のキーデータおよび前記読み出された媒体固有データから中間鍵データを生成し、  
 記録時にユーザーが決めるコンテンツ毎に異なる第3のキーデータを前記中間鍵データで暗号化して第3の暗号化キーデータ生成し、  
 記録するコンテンツを前記第3のキーデータで暗号化して暗号化コンテンツを生成し、  
 前記第3の暗号化キーデータおよび前記暗号化コンテンツを前記記録媒体の書き換え可能な領域に記録し、  
 再生する際には、前記記録媒体から前記媒体固有データを読み出し、  
 前記記録媒体から前記第2の暗号化キーデータを読み出し、  
 前記読み出した前記媒体固有データおよび前記読み出した前記第2の暗号化キーデータから前記第1の暗号化キーデータを復号し、  
 前記第1の暗号化データを復号するために予め割り当てられた前記第2のキーデータ群のいずれかの第2の復号鍵および前記復号された第1の暗号化キーデータを用いて前記第1のキーデータを復号し、  
 前記復号した第1のキーデータおよび前記読み出した媒体固有データより前記中間鍵データを生成し、  
 前記記録媒体の書き換え可能な領域から読み出した前記第3の暗号化キーデータおよび前記中間鍵データを用いて前記第3のキーデータを復号し、  
 前記記録媒体の書き換え可能な領域から読み出した前記暗号化コンテンツおよび前記復号した第3のキーデータを用いて前記コンテンツを復号することを特徴とする記録再生方法。  
 【請求項10】データの書き換え不可能な領域には、予め媒体固有データが記録されており、  
 データの書き換え可能な領域には、第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが予め記録されており、  
 前記書き換え不可能な領域から前記媒体固有データ、前記書き換え可能な領域から第2の暗号化キーデータを伝送し、  
 前記伝送された媒体固有データおよび前記伝送された第2の暗号化キーデータを用いて前記第1の暗号化キーデータを復号し、  
 予め割り当てられた前記第2のキーデータ群のうちのいずれかのキーデータである復号鍵および前記復号された第1の暗号化キーデータを用いて前記第1のキーデータを復号し、

前記復号された前記第1のキーデータおよび前記伝送された媒体固有データから中間鍵データを生成し、  
 前記中間鍵データで記録時にユーザーが決めるコンテンツ毎に異なる第3のキーデータを暗号化して第3の暗号化キーデータ生成し、  
 前記第3のキーデータで前記コンテンツを暗号化して暗号化コンテンツを生成し、  
 前記第3の暗号化キーデータおよび前記暗号化コンテンツを前記書き換え可能な領域に伝送することを特徴とする伝送方法。  
 【請求項11】データの書き換え不可能な領域には、予め媒体固有データが記録されており、  
 データの書き換え可能な領域には、第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが予め記録されており、  
 前記書き換え不可能な領域から前記媒体固有データ、前記書き換え可能な領域から第2の暗号化キーデータを伝送し、  
 前記伝送された媒体固有データおよび前記伝送された第2の暗号化キーデータを用いて前記第1の暗号化キーデータを復号し、  
 予め割り当てられた前記第2のキーデータ群のうちのいずれかのキーデータである第1の復号鍵および前記復号された第1の暗号化キーデータを用いて前記第1のキーデータを復号し、  
 前記復号された前記第1のキーデータおよび前記伝送された媒体固有データから中間鍵データを生成し、  
 前記中間鍵データで記録時にユーザーが決めるコンテンツ毎に異なる第3のキーデータを暗号化して第3の暗号化キーデータ生成し、  
 前記第3のキーデータで前記コンテンツを暗号化して暗号化コンテンツを生成し、  
 前記第3の暗号化キーデータおよび前記暗号化コンテンツを前記書き換え可能な領域に伝送し、  
 前記書き換え不可能な領域から前記媒体固有データ、前記書き換え可能な領域から前記第2の暗号化キーデータ、前記第3の暗号化キーデータおよび前記暗号化コンテンツを伝送し、  
 前記伝送された前記媒体固有データおよび前記伝送された前記第2の暗号化キーデータを用いて前記第1の暗号化キーデータを復号し、  
 予め割り当てられた前記第2のキーデータ群のうちのいずれかのキーデータである第2の復号鍵および前記復号された第1の暗号化キーデータを用いて前記第1のキーデータを復号し、  
 前記復号した第1のキーデータおよび前記伝送された媒体固有データより前記中間鍵データを生成し、  
 前記中間鍵データおよび前記伝送された第3の暗号化キーデータを用いて前記第3のキーデータを復号し、

前記復号した第3のキーデータおよび前記伝送された暗号化コンテンツを用いて前記コンテンツを復号することを特徴とする伝送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、高密度で大容量の記録再生が可能な情報記録媒体に対して相対運動をさせて情報を書き込み、読み出す記録再生装置（ドライブ）に用いられる情報記録媒体、記録装置、記録方法、再生装置、再生方法、記録再生方法、および伝送方法に関する。

【0002】

【従来の技術】情報記録媒体として、DVDが登場しているが、これらに記録されている情報はデジタル情報であるため、デジタル情報が容易にコピーできる状態にあると複製物を劣化なく生成でき、著作権者の権利を侵害するおそれがあるため、コピー防止に関して種々方法が従来提案されている。

【0003】例えば、DVD-Video（読み出し専用）でのコピーガードに関しては、DVDのコピー防止の基本になる方式であるCSS（Content Scramble System）が提案されている。CSSに関しては、例えば、National Technical Report Vol. 43, No. 3, (Jun. 1997) 118頁～122頁「DVD著作権保護システム」等に開示されている。CSSは、デジタル情報をDVDディスクに記録する際にタイトルキー（鍵）、ディスクキー（鍵）、デバイスキー（鍵）の3層の暗号化技術を使用して暗号化し、ライセンスを受けたCSS準拠のDVD機器（プレーヤ）だけが、暗号化されたデジタル情報を復号化して再生可能とするものである。

【0004】上記CSSに関し、DVD-Video（ROM）への適用例について図6を参照して説明する。ディスク製造者（Disc Manufacturer）100は、コンテンツプロバイダーの決めるディスクキー（Disc Key）101を複数のデバイスキー（Device Key）102-1から102-nによりディスクキーブロック処理部（Process DKB）103にて複数のディスクキー群であるディスクキーブロック（DKB）104を生成する。

【0005】これは、複数の機器が持つ異なるデバイスキー（デバイスキー102-1～102-nのうちの一つ）でディスクキー101を復号し利用できるようにするためである。次にDKB104をディスク105上の所定の領域に記録する。次にAVコンテンツを記録する際に決めるタイトル毎に異なるタイトルキー106はタイトルキー暗号化手段107にて、ディスクキー101でスクランブルされ、ディスク105に暗号化タイトルキー（Encryption Title Key）

108として記録される。また、記録されるAVコンテンツ109はコンテンツ暗号化手段（Contents Encryption）110にて、記録する際に決められるタイトル毎に異なるタイトルキー106（スクランブルされる前の）でスクランブルされた暗号化AVコンテンツ（Encrypted AV Contents）109としてディスク105に記録される。ディスク製造者100は、この状態のディスク105を販売する。

【0006】次にディスク105の再生について説明する。再生装置110にもあらかじめ複数のデバイスキー102-1～102-nのうち1つである、例えば、102-jが割り当てられている。再生装置110は再生に先立ち、ディスク2よりディスクキーブロック（DKB）104を読み出し、ディスクキー復号部（Disc Key Decryption）111においてデバイスキー102-jでディスクキーブロック（DKB）104を復号してディスクキー101を得る。次にディスクキー101でスクランブルされ、ディスク105に記録されている暗号化タイトルキー108を読み出し、タイトルキー復号部（Title Key Decryption）112ではディスクキー復号部（Disc Key Decryption）111より出力されるディスクキー101を用いて元々のタイトルキー106を復号する。次に、ディスク105からタイトルキー106でスクランブルされている暗号化AVコンテンツ109を読み出し、コンテンツ復号部（Contents Encryption）113は復号された元々のタイトルキー106を使用してデスクランブルを行いAVコンテンツ109を復元して、AVコンテンツを再生する。

【0007】上述したCSSはDVD-Video（ROM）等の読み出し専用媒体のみに適用可能な方法であり、DVD-RAM、DVD-RW等の書き換え可能な情報記録媒体やDVD-R等の1度だけ書き込みのみ可能な情報記録媒体には適用することはできない。書き換え可能な情報記録媒体であるDVD-RAMに対しては上述したCSSとは別のコピーガードシステムが提案されている。DVD-RAMはROM（読み出し専用）領域とRAM（書き換え可能）領域とをそなえており、コピーガードのキーとなる情報であるDKBはROMの領域に予め記録されているので、重ね書きや改変できない。

【0008】DVD-RAMのコピーガードシステムの概要について図7を参照して説明する。ブランクメディア（記録前の情報記録媒体）に関して説明する。ディスク製造者（Disc Manufacturer）200はディスク（Media）201一枚毎に異なるユニーク・メディア・ID（Unique Media ID）202を記録する。次にコンテンツプロバイダーの決めるディスクキー203を複数のデバイスキー204

1から204-nによりディスクキー暗号化部(Disc Key Encryption)205でスクランブル(暗号化)して複数のディスクキー群であるディスクキーブロック(DKB)206を生成する。これは、複数の機器が持つ異なるデバイスキーでディスクキーを復号し利用できるようにするためである。生成したDKB206は、ユニーク・メディア・ID202と共にディスク201上の所定の領域に記録される。ディスク製造者200は、この状態のディスク201をブランクディスクとして販売する。次にコンテンツの記録について説明する。記録装置207にはあらかじめ複数のデバイスキー204-1~204-nのうち1つデバイスキー204-jが割り当てられている。最初、記録装置207は記録に先立ちディスク201一枚毎にユニークなデータ(ユニーク・メディア・ID)202を読み出す。同様に、ディスク201の所定の領域に記録されているディスクキー群(ディスクキーブロック(DKB)206))を読み出す。記録装置207にあるディスクキー復号部(Disc Key Decryption)208でその装置の持つデバイスキー204-jでディスクキーブロック(DKB)206を復号してディスクキー203を得る。復号されたディスクキー203はユニークメディアキー処理部(Process Unique Media Key)209にて、先に読み出されたユニーク・メディア・ID202で処理され、ディスク201一枚毎にユニークなディスクキー202とされる。

【0009】AVコンテンツを記録する際に決めるタイトル毎に異なるタイトルキー210はタイトルキー暗号化部211にて、ユニークなディスクキー202でスクランブルされ、ディスク201に暗号化タイトルキー(Encryption Title Key)212として記録される。

【0010】また、記録されるAVコンテンツ213はコンテンツ暗号化手段214にて、記録する際に決められるタイトル毎に異なるタイトルキー210でスクランブルされた暗号化AVコンテンツ(Encrypted AV Contents)215としてディスク201に記録される。次に記録されたコンテンツの再生について説明する。再生装置216にもあらかじめ複数のデバイスキー204-1~204-nのうち1つの、例えば、204-kが割り当てられている。ここで、ディスクキーブロック(DKB)206は1つのディスクキー203を複数のデバイスキー204-1~204-nで暗号化(Encrypt)しているので、再生装置216デバイスキー204-kと記録装置のデバイスキー204-jと異なっても復号化等には問題はない。ディスクキー復号部(Disc Key Decryption)217でデバイスキー204-kでディスクキーブロック(DKB)206を復号してディスクキー203

を得る。復号されたディスクキー203は記録側で使ったディスク201一枚毎にユニークなディスクキー202と一致させるため、ディスク201より読み出されたユニーク・メディア・ID202でユニークメディアキー処理部(Process Unique Media Key)218で処理され、ユニークなディスクキー202を得る。次にディスク201に記録されているユニークなディスクキー202でスクランブルされている暗号化タイトルキー212を読み出し、タイトルキー復号部(Title Key Decryption)219にてユニークメディアキー処理部(Process Unique Media Key)218より出力されるユニークなディスクキー202を用いて元々のタイトルキー210を復号する。タイトルキー210でスクランブルされ記録されているAVコンテンツ215をディスク201から読み出し、コンテンツ復号部(Contents Decryption)220において復号された元々のタイトルキー210を使用してデスクランブルを行いAVコンテンツ213を復元してAVコンテンツを再生する。

【0011】ところで、書込みのみ可能な情報記録媒体であるDVD-Rは、ディスクの構造はDVD-RWと同一の構造(メディア上は全てRAM領域)であるが、1度しか記録できない、書き換えできない構造のためDVD-RではDKBの記録はできるが、1度しか記録できないので重ね書きや変造後のデータは利用できなくなり、DVD-RAMと同様なシステムで違法な複製を防止できる。

【0012】

【発明が解決しようとする課題】上述したようにDVD-RAMでは、上述したようにROM領域とRAM領域とを分けて設定してあるので、2つの領域の特性を両立させる事が難しく、性能の両立ができないのでROM領域とRAM領域とをで規格を別々に定義している。従ってDVD-RAMはその構造が特殊で複雑となる。

【0013】DVD-Rはメディア構造が単純なので製造は容易であるが、ただし1度しか記録できないため、記録者の使い勝手は制限される。

【0014】書き換え可能な情報媒体であるDVD-RWでは、DVD-Rのような使用者にとっての制限はないが、DVD-RWのメディア上のデータ記録領域は書き換え可能であるため、DVD-RAMやDVD-Rと同じコピー防止の手法はとれない。つまり、DVD-RWはDVD-RAMの様なROM領域を持たず、DVD-Rの様なライトワンス特性も持たないため、書き換え可能なDVD-RW媒体へのDVD-RAMのコピーガードシステムと同等のコピー防止を従来と同じ手法で実現することができない。

【0015】つまり、例えば、コピーガードの方法として上述したDVD-Rと同一の方法を取るとDVD-R



WではDKB記録部分が書き換え可能であることからデータ重ね書きや変造によりコピーが可能となり、不正な複写を防止することができない。また、DVD-RAMの様なROM領域をつくるにしても、DVD-RWでは記録前の空溝特性とROM領域を実現するためのEmboss Pitとを両立させる事が難しい。どちらかの性能を優先させると他方の性能を十分設定することができない等の矛盾が生じるため、有効なコピー防止を実現することができないという問題点を有していた。

【0016】

【課題を解決するための手段】本発明は、上述の問題点を解決するために、媒体固有データが記録された書き換え不可能な非データ領域である第1の領域と、第1のキーデータを第2のキーデータで暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが記録されている第2の領域と、ユーザデータの記録領域である書き換え可能な第3の領域とを有することを特徴とする情報記録媒体を提供する。また、本発明は、上述の問題点を解決するために媒体固有データが記録された書き換え不可能な非データ領域と、第1のキーデータを第2のキーデータで暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータ、およびユーザデータが記録される書き換え可能な領域とを有することを特徴とする情報記録媒体を提供する。また、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録する記録装置であって、前記第1の暗号化キーデータから前記第1のキーデータを復号するために予め割り当てられた前記第2のキーデータ群のうちのいずれかの復号鍵を記憶する記憶手段と、前記情報記録媒体から前記媒体固有データを読み出す手段と、前記情報記録媒体から前記第2の暗号化キーデータを読み出す手段と、前記読み出した媒体固有データおよび前記読み出した第2の暗号化キーデータを用いて前記第1の暗号化キーデータを復号する第1の復号手段と、前記復号鍵および前記復号された第1の暗号化キーデータを用いて前記第1のキーデータを復号する第2の復号手段と、前記復号された第1のキーデータおよび前記読み出された媒体固有データから中間鍵データを生成する手段と、記録時にユーザーが決める前記コンテンツ毎に異なる第3のキーデータを前記中間鍵データで暗号化する第1の暗号化手段と、記録する前記コンテンツを前記第3のキーデータで暗号化する第2の暗号化手段と、前記第1の暗号化手段で暗号化された前記第3のキーデータおよび前記第2

の暗号化手段で暗号化された前記コンテンツを前記情報記録媒体の前記書き換え可能な領域に記録する記録手段とを有することを特徴とする記録装置を提供する。また、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録する記録方法であって、前記記録媒体から前記媒体固有データを読み出し、前記記録媒体から前記第2の暗号化キーデータを読み出し、前記読み出した媒体固有データおよび前記読み出した第2の暗号化キーデータを用いて前記第1の暗号化キーデータを復号し、前記第1の暗号化キーデータを復号するために予め割り当てられた前記第2のキーデータ群のうちのいずれかの復号鍵で前記第1の暗号化キーデータを復号して前記第1のキーデータを復号し、前記復号された前記第1のキーデータおよび前記媒体固有データから中間鍵データを生成し、記録時にユーザーが決める前記コンテンツ毎に異なる第3のキーデータを前記中間鍵データで第3の暗号化キーデータを生成し、記録する前記コンテンツを前記第3の暗号化キーデータで暗号化して暗号化コンテンツを生成し、前記第3の暗号化キーデータおよび前記暗号化コンテンツを前記情報記録媒体の前記書き換え可能な領域に記録することを特徴とする記録方法を提供する。また、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体であって、コンテンツの記録時に、前記第2の暗号化キーデータを前記媒体固有データで復号した前記第1の暗号化キーデータを、さらに予め割り当てられた前記第2のキーデータ群のうちのいずれかの復号鍵で復号した前記第1のキーデータおよび前記媒体固有データを用いて生成した中間鍵データで記録時にユーザーが決めるコンテンツ毎に異なる第3のキーデータを暗号化した第3の暗号化キーデータと、前記第3のキーデータを鍵として前記コンテンツを暗号化した暗号化コンテンツとが前記書き換え可能な領域に記録されていることを特徴とする情報記録媒体を提供する。また、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを、さらに前記媒体



固有データで暗号化した第2の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録するにあたり、前記第2の暗号化キーデータを前記媒体固有データで復号した前記第1の暗号化キーデータを予め割り当てられた前記第2のキーデータ群のうちのいずれかの第1の復号鍵で復号された前記第1のキーデータおよび前記媒体固有データを用いて生成した中間鍵データで、記録時にユーザーが決めるコンテンツ毎に異なる第3のキーデータを暗号化した第3の暗号化キーデータと、前記第3のキーデータを鍵として前記コンテンツを暗号化した暗号化コンテンツとが前記書き換え可能な領域に記録されている情報記録媒体より前記コンテンツを再生する再生装置であって、前記第1の暗号化キーデータから前記第1のキーデータを復号するために予め割り当てられた前記第2のキーデータ群のうちのいずれかの第2の復号鍵を記憶する記憶手段と、前記情報記録媒体から前記媒体固有データを読み出す手段と、前記情報記録媒体から前記第2の暗号化キーデータを読み出す手段と、前記読み出した媒体固有データおよび前記読み出した第2の暗号化キーデータを用いて前記第1の暗号化キーデータを復号する第1の復号手段と、前記第2の復号鍵および前記復号した第1の暗号化キーデータを用いて前記第1のキーデータを復号する第2の復号手段と、前記復号した第1のキーデータおよび前記読み出した媒体固有データから前記中間鍵データを生成する手段と、前記書き換え可能な領域から前記第3の暗号化キーデータを読み出し、前記読み出した第3の暗号化キーデータおよび前記中間鍵データを用いて前記第3のキーデータを復号する第3の復号手段と、前記書き換え可能な領域から前記暗号化コンテンツを読み出し、前記第3の復号化手段で復号された前記第3のキーデータおよび前記暗号化コンテンツを用いて前記コンテンツを復号する第4の復号手段とからなることを特徴とする再生装置を提供する。また、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録するにあたり、前記第2の暗号化キーデータを前記媒体固有データで復号した前記第1の暗号化キーデータを前記第2のキーデータ群のうちのいずれかの第1の復号鍵で復号された前記第1のキーデータおよび前記媒体固有データを用いて生成した中間鍵データで、記録時にユーザーが決めるコンテンツ毎に異なる第3のキーデータを暗号化した第3の暗号化キーデータと、前記第3のキーデータを鍵として前記コンテンツを暗号化した暗号化コンテンツとが前記書き換え可能な領域に記録されている情報記

録媒体より前記コンテンツを再生する再生方法であって、前記情報記録媒体から前記媒体固有データを読み出し、前記情報記録媒体から前記第2の暗号化キーデータを読み出し、前記読み出した媒体固有データおよび前記読み出した第2の暗号化キーデータから前記第1の暗号化キーデータを復号し、前記第1の暗号化キーデータを復号するために予め割り当てられた前記第2のキーデータ群のうちのいずれかの第2の復号鍵および前記第1の暗号化キーデータを用いて前記第1のキーデータを復号し、前記復号した第1のキーデータおよび前記読み出した媒体固有データから前記中間鍵データを生成し、前記中間鍵データおよび前記第3の暗号化キーデータを用いて前記第3のキーデータを復号し、前記書き換え可能な領域から前記暗号化コンテンツを読み出し、前記復号した前記第3のキーデータおよび前記暗号化コンテンツを用いて前記コンテンツを復号することを特徴とする再生方法を提供する。また、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域と、データの書き換え可能な領域とを有し、前記書き換え不可能な領域には媒体固有データが記録され、前記書き換え可能な領域には第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを前記媒体固有データで暗号化した第2の暗号化キーデータが予め記録された情報記録媒体を用いた記録再生方法であって、記録する際には、前記記録媒体より前記媒体固有データを読み出し、前記記録媒体から前記第2の暗号化キーデータを読み出し、前記読み出した媒体固有データおよび前記読み出した第2の暗号化キーデータを用いて前記第1の暗号化キーデータを復号し、前記第1の暗号化キーデータを復号するために予め割り当てられている前記第2のキーデータ群のいずれかの復号鍵および前記復号された第1の暗号化キーデータを用いて前記第1のキーデータを復号し、前記復号された前記第1のキーデータおよび前記読み出された媒体固有データから中間鍵データを生成し、記録時にユーザーが決めるコンテンツ毎に異なる第3のキーデータを前記中間鍵データで暗号化して第3の暗号化キーデータ生成し、記録するコンテンツを前記第3のキーデータで暗号化して暗号化コンテンツを生成し、前記第3の暗号化キーデータおよび前記暗号化コンテンツを前記記録媒体の書き換え可能な領域に記録し、再生する際には、前記記録媒体から前記媒体固有データを読み出し、前記記録媒体から前記第2の暗号化キーデータを読み出し、前記読み出した前記媒体固有データおよび前記読み出した前記第2の暗号化キーデータから前記第1の暗号化キーデータを復号し、前記第1の暗号化データを復号するために予め割り当てられた前記第2のキーデータ群のいずれかの第2の復号鍵および前記復号された第1の暗号化キーデータを用いて前記第1のキーデータを復号し、前記復号した第1のキーデータおよび前記読み出した媒体固有データより前記中間鍵データを

生成し、前記記録媒体の書き換え可能な領域から読み出した前記第3の暗号化キーデータおよび前記中間鍵データを用いて前記第3のキーデータを復号し、前記記録媒体の書き換え可能な領域から読み出した前記暗号化コンテンツおよび前記復号した第3のキーデータを用いて前記コンテンツを復号することを特徴とする記録再生方法を提供する。また、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域には、予め媒体固有データが記録されており、データの書き換え可能な領域には、第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが予め記録されており、前記書き換え不可能な領域から前記媒体固有データ、前記書き換え可能な領域から第2の暗号化キーデータを伝送し、前記伝送された媒体固有データおよび前記伝送された第2の暗号化キーデータを用いて前記第1の暗号化キーデータを復号し、予め割り当てられた前記第2のキーデータ群のうちのいずれかのキーデータである復号鍵および前記復号された第1の暗号化キーデータを用いて前記第1のキーデータを復号し、前記復号された前記第1のキーデータおよび前記伝送された媒体固有データから中間鍵データを生成し、前記中間鍵データで記録時にユーザーが決めるコンテンツ毎に異なる第3のキーデータを暗号化して第3の暗号化キーデータ生成し、前記第3のキーデータで前記コンテンツを暗号化して暗号化コンテンツを生成し、前記第3の暗号化キーデータおよび前記暗号化コンテンツを前記書き換え可能な領域に伝送することを特徴とする伝送方法を提供する。さらに、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域には、予め媒体固有データが記録されており、データの書き換え可能な領域には、第1のキーデータを複数の第2のキーデータ群で暗号化した第1の暗号化キーデータを、さらに前記媒体固有データで暗号化した第2の暗号化キーデータが予め記録されており、前記書き換え不可能な領域から前記媒体固有データ、前記書き換え可能な領域から第2の暗号化キーデータを伝送し、前記伝送された媒体固有データおよび前記伝送された第2の暗号化キーデータを用いて前記第1の暗号化キーデータを復号し、予め割り当てられた前記第2のキーデータ群のうちのいずれかのキーデータである第1の復号鍵および前記復号された第1の暗号化キーデータを用いて前記第1のキーデータを復号し、前記復号された前記第1のキーデータおよび前記伝送された媒体固有データから中間鍵データを生成し、前記中間鍵データで記録時にユーザーが決めるコンテンツ毎に異なる第3のキーデータを暗号化して第3の暗号化キーデータ生成し、前記第3のキーデータで前記コンテンツを暗号化して暗号化コンテンツを生成し、前記第3の暗号化キーデータおよび前記暗号化コンテンツを前記書き換え可能な領域に伝送し、前記書き換え不可能な領

域から前記媒体固有データ、前記書き換え可能な領域から前記第2の暗号化キーデータ、前記第3の暗号化キーデータおよび前記暗号化コンテンツを伝送し、前記伝送された前記媒体固有データおよび前記伝送された前記第2の暗号化キーデータを用いて前記第1の暗号化キーデータを復号し、予め割り当てられた前記第2のキーデータ群のうちのいずれかのキーデータである第2の復号鍵および前記復号された第1の暗号化キーデータを用いて前記第1のキーデータを復号し、前記復号した第1のキーデータおよび前記伝送された媒体固有データより前記中間鍵データを生成し、前記中間鍵データおよび前記伝送された第3の暗号化キーデータを用いて前記第3のキーデータを復号し、前記復号した第3のキーデータおよび前記伝送された暗号化コンテンツを用いて前記コンテンツを復号することを特徴とする伝送方法を提供する。

【0017】

【発明の実施の形態】本発明は、メディア上のDKBをディスク毎に変えて、ディスク毎に異なるUnique Media IDを利用して暗号化したDKBを生成して記録することにより、例えば、DKB領域を含むディスク丸ごとコピーが行われたとしても、ディスク毎にIDが異なるため、記録されているコンテンツを再生することが不可能となり、不正な複製を防止することが可能となる。またメディア上のDKBが重ね書きや改変された場合にもコンテンツの復号に必要なキーが正しく復元できなくなるので不正な複製は防止される。

【0018】上述したようにReadable Emboss-pitを現状では記録する技術が確立していないDVD-RWに従来方式のDKB記録によるコピーガードを実現するため、DVD-RWのリードイン領域のSystem Reserved領域に、従来方式のDKBをメディア固有のUnique Media IDを使いさらに暗号化し、メディア個々に異なる暗号化DKBを記録する。ディスク製造者はDKBをUnique Media IDで暗号化し、工場出荷時に暗号化DKBをディスクに記録(Pre-record)し、出荷する。

【0019】記録装置はUnique Media IDと暗号化DKBを読み出しDKBを復元し従来方式により記録し、再生装置は同様にUnique Media IDと暗号化DKBとを読み出しDKBを復元して再生する。

【0020】例えば、図8に示すようにUnique Media ID Aのディスクでは暗号化DKB Aが生成されディスクに記録されているので、暗号化DKBを復号する際にはディスクにUnique Media ID Aが記録されていることが必要である。しかし、このディスクをビット・バイ・ビットでUnique Media ID Bのディスクに記録した場合は、暗号化DKBを復号する際にディスクに記録されて

いるUnique Media ID Bが使用されるため正しい復号ができなくなる。

【0021】図9に示すようにディスク2にはその最内周部よりリードイン領域(Lead-in Area)、ユーザデータ領域(User Data Area)が順次配置されている。リードイン領域は記録再生の際の制御に使用されるデータを格納する領域であり、ユーザデータ領域は記録再生されるべきコンテンツを暗号化した暗号化コンテンツ(データ)を配置する領域である。

【0022】リードイン領域は読み出し専用(書き換え不可能な領域)のBCA領域(BCA Area)、読み出し/書き込みが可能(書き換え可能な領域)なシステムリザーブ領域(System reserved Area)、読み出し専用(書き換え不可能な領域)のコントロールデータ領域(Control Data Area)から構成されている。BCA領域には、BCAに関するデータ、つまり、ディスク2の1枚毎に異なるデータである上述したUnique Media IDが記録されている。リザーブ領域は著作権やコピープロテクトに関する情報(データ)を記録するために用意されている領域であり、例えば、メディア固有のUnique Media ID(BCA)を用いて暗号化することにより生成されるディスク2の個々に異なる暗号化DKBを記録する。

【0023】なお、この暗号化DKBはリザーブ領域ではなく、ユーザデータ領域(書き換え可能な領域)に記録することも可能であり、また、リザーブ領域およびユーザデータ領域の両方の領域に記録してもよい。ユーザデータ領域に記録する場合は、その記録位置はリードイン領域の直後、ユーザデータ領域の最後、ユーザデータ領域の中の任意の位置などユーザデータ領域の所定の位置であり、更に複数の所定の位置に記録することも可能である。このようなユーザデータ領域への格納とリザーブ領域への格納とを併存させることも可能である。

【0024】以下、本発明の実施例に関して図面を用いて詳しく説明する。図1は本発明の実施例を示す図である。

#### (1) ブランクメディア

まず、ブランクメディア(コンテンツが記録される前の情報記録媒体)に関して説明する。ディスク製造者(Disc Manufacturer)1はディスク(Media)2一枚毎にユニーク・メディア・データ(Unique Media ID)3をディスクに記録する。

【0025】ユニーク・メディア・データ3を記録する際に、コンテンツプロバイダーの決めるディスクキー4を複数のデバイスキー5-1から5-nによりディスクキー暗号化部(Disc Key Encryption)6でスクランブル(暗号化)して複数のディスクキ

一群であるディスクキーブロック(DKB)7を生成する。これは、複数の機器が持つ異なるデバイスキーでディスクキーを復号し利用できるようにするためである。

【0026】なお、上記説明におけるスクランブルに関する処理は、例えば、図2に示すようなスクランブラー300にて行うことができる。具体的にはキーデータを初期値にM系列のPN乱数をPN乱数発生手段301にて発生させ、スクランブルしたい入力データとEOR手段302にてEX-OR(排他的論理和)をとることで処理を行う。図1に示した実施例では、キーデータとして図1に示した複数のデバイスキー5-1~5-nを初期値としてPN乱数発生手段301入力してPN乱数を発生させ、スクランブルしたいデータであるディスクキー4とPN乱数とのEX-OR(排他的論理和)処理をEOR手段302で行うことでディスクキー4をスクランブル処理することができる。なお、以下の説明でのスクランブル処理に関しても図2に示したスクランブラー300を使用して処理することが可能である。

【0027】なお、上述したPN乱数発生手段301に関しては、例えば、図4に示すようなPN乱数発生部500を使用することができる。PN乱数発生部500はDフリップフロップ501、502、503、504を4回路を従属接続し、初期値をバラレルデータとしてDフリップフロップ501、502、503、504に供給し、シリアル形式のPN乱数を得ることができる。

【0028】さらに詳細に説明すると、PN乱数発生手段301はM系列(最長線型符号系列)を用いた疑似乱数発生回路で、回路はある長さのシフトレジスターまたは遅延素子(実施例では4ビットのD-FF)と複数のレジスターの状態を演算してレジスターの入力に帰還する回路(実施例ではEORと反転回路)により構成される。

【0029】M系列は後述するようにレジスターへの初期値および帰還回路の構成によりレジスターのクロック毎に出力に現れるビットパターンが異なり、最長 $2^n - 1$ (2のn乗-1)の周期を持つ疑似乱数パターンが得られる。この特性を生かして本願の様なデータのスクランブルを始め通信分野(スペクトラム拡散方式など)に多用されている。

【0030】上述した図4に示したPN乱数発生手段301はPN符号長15クロックで、例えばレジスターの初期値に「0000」binをロードしてクロック毎にレジスターをビットシフトすると、その出力には図10に示すように0に始まり15クロックを1周期とする疑似乱数が得られる。また「1001」binをロードしてクロック毎にレジスターをビットシフトすると、その出力には図11に示すように1に始まり15クロックを1周期とする表-1とは異なるパターンの疑似乱数が得られる。

【0031】このようにして得られた疑似乱数を図2に

示したスクランブラー 300 に用いれば同じ入力データであっても出力されるデータは図 10 および図 11 に示すように PN 乱数発生手段 301 の初期値によって異なり、図 3 のデスクランブラー 400 ので PN 乱数発生手段 401 の初期値と帰還回路の構成を知らないと、正しく元のデータを復元する事はできない。これによりデータを秘匿する事が可能になる。

【0032】また上述した実施例では PN 乱数発生手段 301 のレジスタ長を 4 ビットとしたので疑似乱数の発生周期は 15 クロックであるが、レジスタ長を更に長く、例えば、40 ビットや 64 ビットにする事で PN 乱数発生手段 301 のパターン周期は飛躍的に長くなり、出力される疑似乱数のパターンもより複雑で長周期となり、スクランブラー 300 の出力はさらに解読しにくくなり、秘匿性が高まる。

【0033】ディスク 2 一枚毎にユニークなディスクキー群を作るため、ディスク 2 に記録されたディスク 2 一枚毎にユニークなデータ (ユニーク・メディア・ID) 3 を使用してスクランブルされた複数のディスクキー群 (ディスクキーブロック (DKB)) 7 を暗号化手段 (Encryption) 8 にて再度スクランブルしてこの二重にスクランブルされた複数のディスクキー群である暗号化 DKB (Encrypted DKB) 9 をディスク 2 上の所定の領域に記録する。このスクランブル処理は、例えば、上述した図 2 に示すようなスクランブラー 300 を使用することができる。ディスク製造者 1 は、この状態のディスク 2 をブランクディスクとして販売する。

#### 【0034】(2) 記録装置

記録装置 10 にはあらかじめ複数のデバイスキー 5-1 ~ 5-n のうち 1 つデバイスキー 14 (5-j) が割り当てられており、例えば、メモリ等の記憶手段に記憶されている。記録装置 10 は記録に先立ちディスク 2 の所定領域に記録されているディスク 2 一枚毎にユニークなデータ (ユニーク・メディア・ID) 3 を読み出すと共に、ディスク 2 の所定の領域に記録されている暗号化 DKB 9 を読み出す。

【0035】記録装置 10 のスクランブルディスクキー復号手段 (DKB Decryption) 11 では、ディスク 2 より読み出した暗号化 DKB 9 を、ディスク 2 より読み出したユニーク・メディア・ID 3 でデスクランブルしてディスクキー群 (ディスクキーブロック (DKB 12)) を得る。なお、上記説明におけるデスクランブル処理は、例えば、図 3 に示すようなデスクランブラー 400 で行うことができる。デスクランブラー 400 は図 2 に示したスクランブラー 300 と同様にキーデータを初期値に PN 乱数発生部 401 にて M 系列の PN 乱数を発生させ、デスクランブルしたいデータと PN 乱数とを EX-OR (排他的論理和) 処理を実行すればデータを復元 (デスクラン

ブル処理) することができる。

【0036】図 1 に示した実施例では、キーデータとして図 1 に示したユニーク・メディア・ID 3 を初期値として PN 乱数発生手段 401 入力して PN 乱数を発生させ、デスクランブルしたいデータである暗号化 DKB 9 と PN 乱数との EX-OR (排他的論理和) 処理を EX-OR 手段 402 で行うことで暗号化 DKB 9 をデスクランブル処理して DKB 12 を復元することができる。なお、以下の説明でのデスクランブル処理に関しても図 3 に示したデスクランブラー 400 を使用して処理することが可能である。また、上述した PN 乱数発生部 401 に関しては、上述したように、例えば、図 4 に示した PN 乱数発生部 500 を使用することができる。

【0037】次に記録装置 10 にあるディスクキー復号手段 (Disc Key Decryption) 13 で記録装置 10 の持つデバイスキー 14 でディスクキーブロック (DKB) 12 (DKB 7 に相当) を復号 (デスクランブル) してディスクキー 15 (ディスクキー 4 に相当) を得る。このデスクランブル処理にも、例えば、上述した図 3 に示したデスクランブラー 300 を使用することが可能である。

【0038】復号されたディスクキー 15 はユニークメディアキー処理部 (Process Unique Media Key) 16 にて、先にディスク 2 より読み出されたユニーク・メディア・ID 3 で処理され、ディスク 2 一枚毎にユニークなディスクキー 17 とされる。具体的には、例えば、図 5 に示すようにディスクキー復号部 13 より出力されるディスクキー 15 を鍵情報として EX-OR 601 に入力すると共に、ディスク 2 より再生されたユニーク・メディア・ID 3 を媒体識別情報として EX-OR 601 に入力して EX-OR (排他的論理和) 処理を実行することで、ユニークなディスクキー 17 が出力される。

【0039】タイトルキー暗号化手段 19 において、AV コンテンツを記録する際に決めるタイトル毎に異なるタイトルキー 18 は、ユニークなディスクキー 17 でスクランブルされ、ディスク 2 に暗号化タイトルキー (Encrypted Title Key) 20 として記録される。なお、スクランブル処理に関しては例えば、上述した図 2 に示したスクランブラー 200 を適用可能である。

【0040】また、記録される AV コンテンツ 21 はコンテンツ暗号化手段 22 にて、記録する際に決められるタイトル毎に異なるタイトルキー 18 (スクランブルされる前の) でスクランブルされた暗号化 AV コンテンツ (Encrypted AV Contents) 31 としてディスク 2 に記録される。なお、スクランブル処理に関しては例えば、上述した図 2 に示したスクランブラー 200 を適用可能である。

#### 【0041】(3) 再生装置

再生装置 23 にもあらかじめ複数のデバイスキー 5-1 ~ 5-n のうち 1 つ、例えば、デバイスキー 24 ( 5-k ) が割り当てられている。上述したようにディスクキーブロック ( DKB7 ) は 1 つのディスクキー 4 を複数のデバイスキー 5-1 ~ 5-n で暗号化 ( Encrypt ) しているので再生装置 23 のデバイスキー 24 ( 5-k ) は、記録装置のデバイスキー 14 ( 5-j ) と異なるデバイスキーでかわらない。

【 0042 】再生装置 23 は再生に先立ち、ディスク 2 一枚毎にユニークなデータ ( ユニーク・メディア・ID ) 3 を読み出すと共に、ディスク 2 の所定の領域に記録されている暗号化 DKB9 を読み出す。

【 0043 】再生装置 23 にあるスクランブルディスクキー復号部 ( DKB Decryption ) 25 では、ディスク 2 より読み出した二重にスクランブルされたディスクキー群 9 を、同じくディスク 2 より読み出したユニーク・メディア・ID 3 でデスクランブルしてディスクキー群 ( ディスクキーブロック ( DKB ) ) 26 ( DKB7 に相当 ) を復元する。なお、上述したデスクランブルの処理には、例えば、上述した図 3 に示したデスクランブラー 300 を適用することが可能である。

【 0044 】次に再生装置 23 にあるディスクキー復号部 ( Disc Key Decryption ) 27 で再生装置 23 の持つデバイスキー 24 でディスクキーブロック ( DKB ) 26 を復号してディスクキー 28 ( ディスクキー 4 に相当 ) を復元する。

【 0045 】復号されたディスクキー 28 は記録側で使ったディスク 2 一枚毎にユニークなディスクキー 17 と一致させるため、ディスク 2 より読み出されたユニーク・メディア・ID 3 を用いてユニークメディアキー処理部 ( Process Unique Media Key ) 29 で処理され、ユニークなディスクキー 17 を得る。この処理には、例えば、上述した図 5 に示した EOR601 による処理を適用することが可能である。この場合、鍵情報としてディスクキー 28 を、媒体識別情報としてユニーク・メディア・ID 3 を EOR601 に入力することによりユニークなディスクキー 17 を復元することができる。

【 0046 】次にディスク 2 に記録されている暗号化タイトルキー 20 を読み出す。暗号化タイトルキー 20 はユニークなディスクキー 17 で暗号化されているので、ユニークメディアキー処理部 ( Process Unique Media Key ) 29 より出力されるユニークなディスクキー 17 を使ってタイトルキー復号部 ( Title Key Decryption ) 30 において、暗号化タイトルキー 20 を元々のタイトルキー 18 に復号する。

【 0047 】ディスク 2 から暗号化 AV コンテンツ 31 を読み出し、暗号化 AV コンテンツ 31 はタイトルキー 18 でスクランブルされているので、コンテンツ復号部

( Contents Encryption ) 32 は復号されたタイトルキー 18 を使用してデスクランブルを行い AV コンテンツ 21 を得る。

【 0048 】なお、上記説明におけるでスクランブラーはキーデータを初期値に M 系列の乱数を発生させスクランブルしたいデータと EOR をとることで処理を行う。これに対してデスクランブラーはスクランブラーと同様にキーデータを初期値に M 系列の乱数を発生させスクランブルしたいデータと EOR をとれば、M 系列のデータはスクランブラーと同期がとれるためデータを復元することができる。また、ディスクキーをディスク一枚毎に異なるユニーク・メディア・ID と EOR をとればユニークなディスクキーが得られる。

【 0049 】本発明は上述したようにディスク一枚毎にユニークなデータ ( ユニーク・メディア・ID ) が記録され、その ID でスクランブルされた複数のディスクキー群 ( DKB ) が二重にスクランブルされているので、メディア上のスクランブルされた DKB データはディスク毎に異なる。したがって、データとして記録されたスクランブルされたコンテンツデータやタイトルキーデータがスクランブルされた DKB データを含んで別のディスクにディスク丸ごとコピーが行われたとしても、コピー先のユニーク・メディア・ID はコピー元のユニーク・メディア・ID と全く異なるため正しくディスクキーブロックは復元できない。正しくディスクキーブロックが復元できないとタイトルキーデータやスクランブルされたコンテンツデータは復元できないのでコピー防止になる。

【 0050 】DVD-RAM と異なり DVD-RW の MKB 記録領域は書き換え可能であるが、そこに書かれている二重に暗号化されたディスクキーブロックを改変するとしても、ユニーク・メディア・ID と二重に暗号化されたディスクキーブロックの関係 ( 暗号のアルゴリズム ) がわからない限り正しく改変されたディスクキーブロックデータは得られない。つまりメディア上は全ての領域で書き換え可能な DVD-RW 媒体で技術的見通しが立っていない Emboss-pitt を使わずに DVD-RAM と同じコピー防止が実現できる。

【 0051 】本発明は上述したような構成であるので、DVD-RAM の様な ROM の領域と RAM の領域の性能を両立させ、かつ性能の両立をさせるような特殊な構造のメディアとする必要が無く、メディア上は全ての領域で書き換え可能な ( Unique Media ID 領域を除き ) ままで書き換え可能な媒体のコピー防止が実現でき、またメディア上は全ての領域で書き換え可能な領域なので、ROM の領域と RAM の領域で規格を分ける必要も無く、さらに、例えば、BCA 等の Unique Media ID によりディスクキーブロックが二重にスクランブルされたデータはディスク毎に異なるので、DKB 領域を含むディスク丸ごとコピーが行われ

でも正しくディスクキーブロックは復元できないのでコンテンツデータは復元できない。つまり、一枚一枚のディスクに記録されるのはスクランブルされたDKBだから従来のような裸のDKBデータを記録する場合に比べてハッキングに対する強度が増す。さらに、ディスクキーブロックを使用しているので記録機、再生機でデバイスキーが異なっても構わない。

【0052】

【発明の効果】本発明は上述したような構成であるので、書き換え可能な媒体のコピー防止を実現でき、記録されたデータはディスク毎に異なるのでディスク丸ごとコピーが行われたとしてもコンテンツデータは正しく復元できないので、強力なコピープロテクトが可能となり、さらに、ディスクキーブロックを使用しているので記録機、再生機でデバイスキーが異なっても正規の再生は可能になるという利点を有する。

【0053】

【図面の簡単な説明】

【図1】本発明の実施例を示す図である。

【図2】スクランブラーの一例を示す図である。

【図3】デスクランブラーの一例を示す図である。

【図4】PN乱数発生部の一例を示す図である。

【図5】演算処理の一例を示す図である。

【図6】CSSのDVD-Video (ROM) への適用例を示す図である。

【図7】DVD-RAMのコピーガードを説明する図である。

【図8】ビットバイビットコピーを説明するための図である。

【図9】ディスクの物理レイアウトを示す図である。

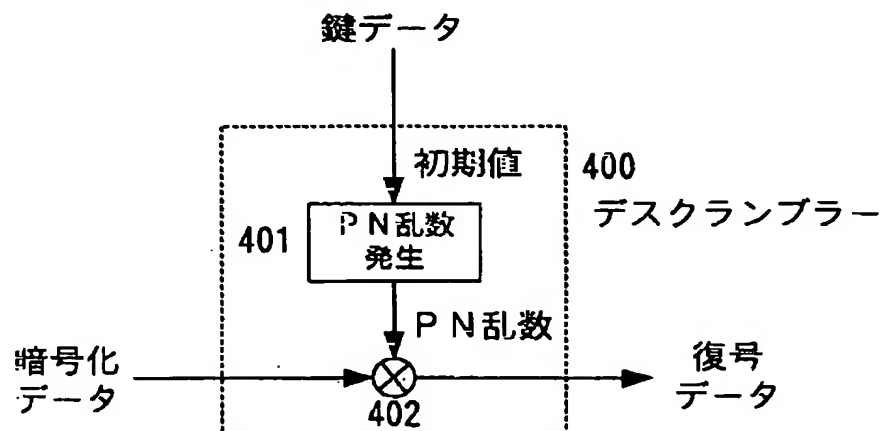
【図10】初期値「0000」のときのPN乱数発生手段301の出力を示す図である。

【図11】初期値「1001」のときのPN乱数発生手段301の出力を示す図である。

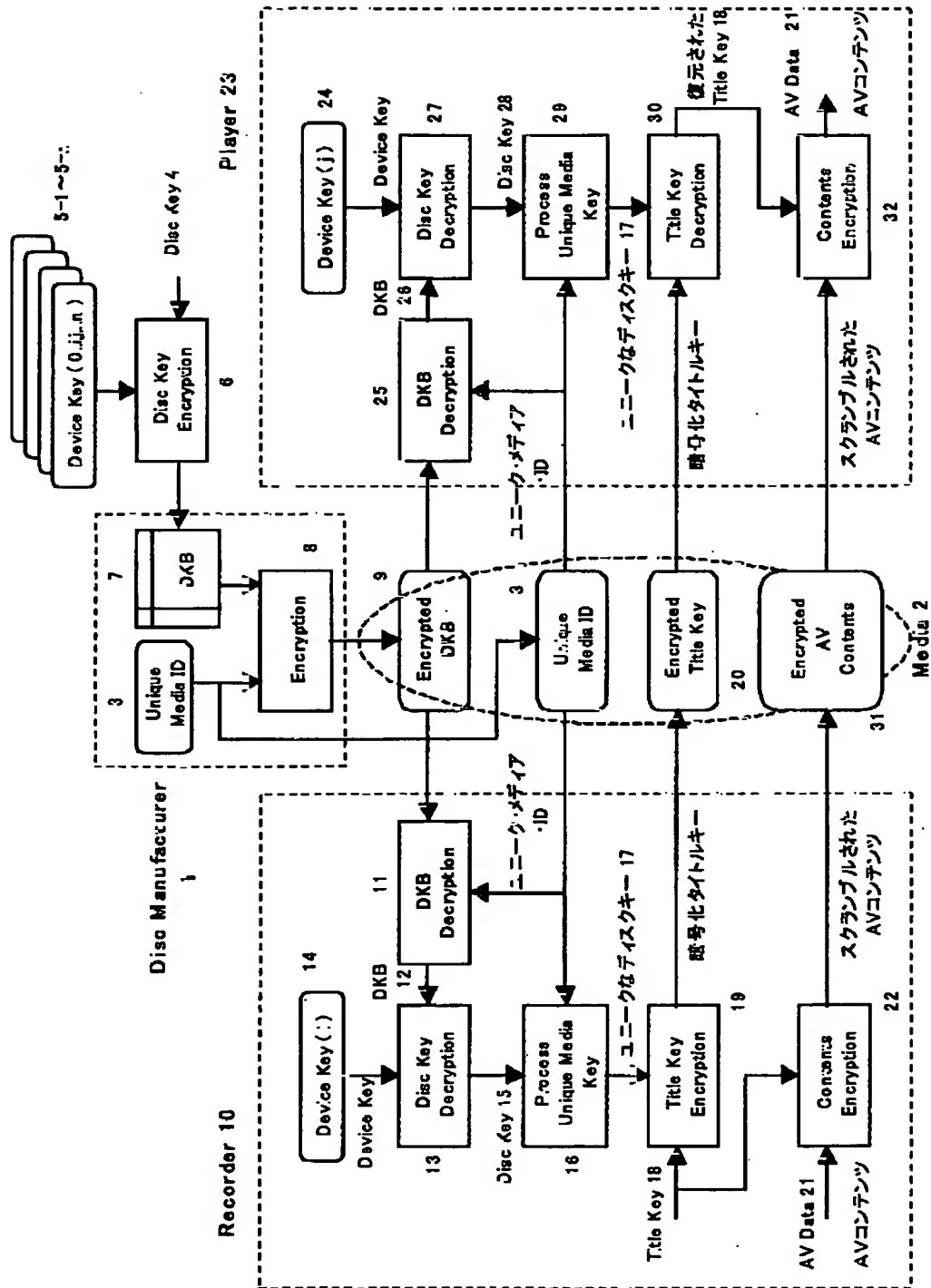
【符号の説明】

- 1…ディスク製造者
- 2…ディスク
- 3…ユニーク・メディア・ID
- 4…ディスクキー
- 5-1～5-n…デバイスキー
- 6…ディスクキー暗号化手段
- 7…ディスクキーブロック (DKB)
- 8…暗号手段
- 9…暗号化DKB
- 10…記録機
- 11…DKB復号手段
- 12…DKB
- 13…ディスクキー復号手段
- 14…デバイスキー
- 15…ディスクキー
- 16…ユニークメディアキー処理手段
- 17…ユニークディスクキー
- 18…タイトルキー
- 19…タイトル暗号手段
- 20…暗号化タイトルキー
- 21…AVコンテンツ
- 22…コンテンツ暗号手段
- 23…再生機
- 24…デバイスキー
- 25…DKB復号手段
- 26…DKB
- 27…ディスクキー復号手段
- 28…ディスクキー
- 29…ユニークメディアキー処理手段
- 30…タイトルキー復号手段
- 31…暗号化AVコンテンツ
- 32…AVコンテンツ復号手段

【図3】

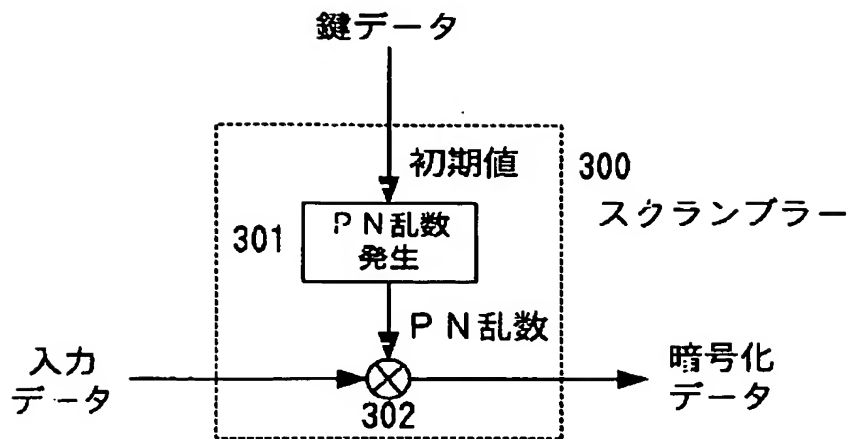


【 図 1 】





【図2】



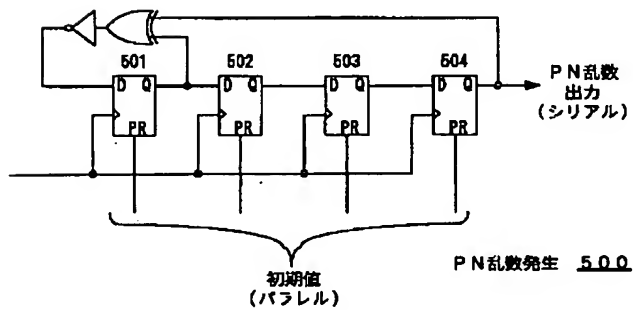
【図10】

初期値 = 「0000」

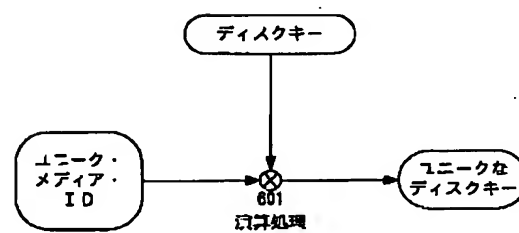
クロック数	レジスタ値	出力	データ	スクランブル出力
0	0000	0	0	0
1	1000	0	0	0
2	0100	0	0	0
3	1010	0	0	0
4	0101	1	1	0
5	0010	0	0	0
6	1001	1	0	1
7	1100	0	0	0
8	0110	0	0	0
9	1011	1	1	0
10	1101	1	0	1
11	1110	0	0	0
12	0111	1	1	0
13	0011	1	1	0
14	0001	1	0	1
15	0000	0	0	0
16	1000	0	0	0
17	0100	0	0	0
18	1010	0	1	1
19	0101	1	0	1
20	0010	0	1	1
21	1001	1	0	1
22	1100	0	1	1
23	0110	0	0	0

MSB

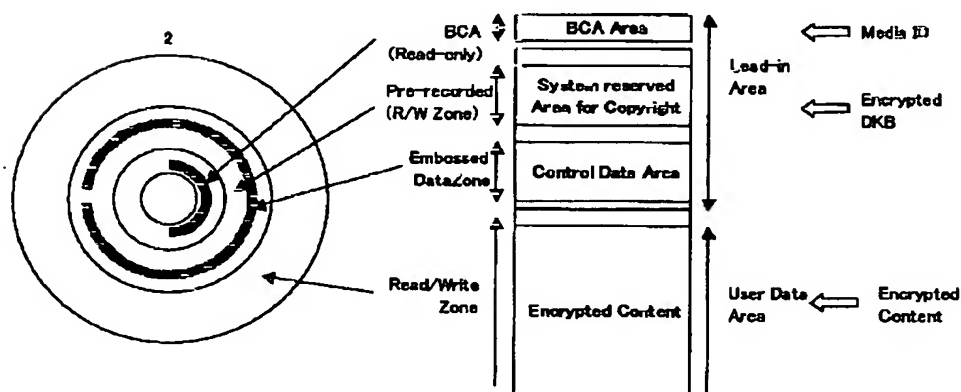
【図4】



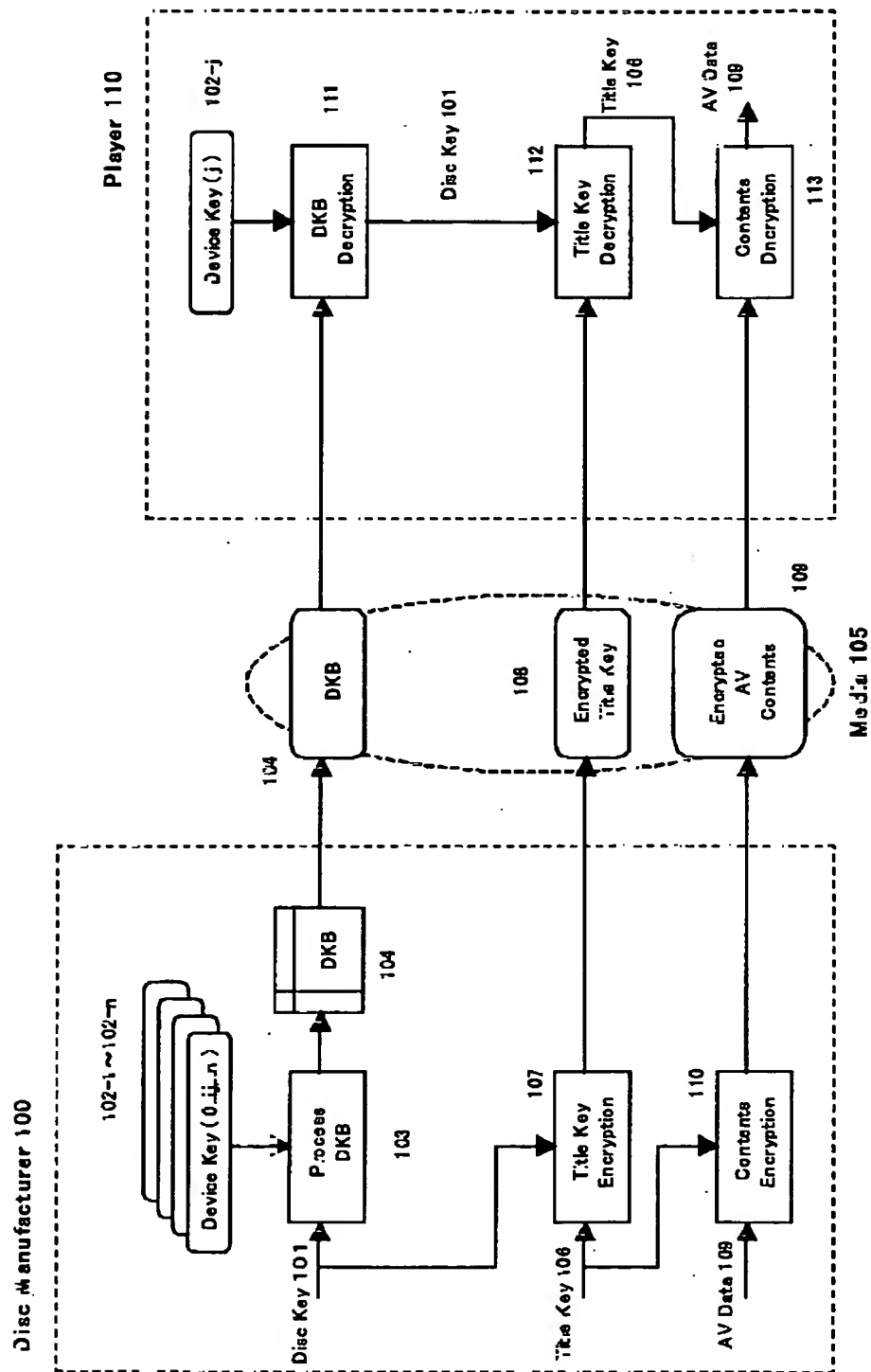
【図5】



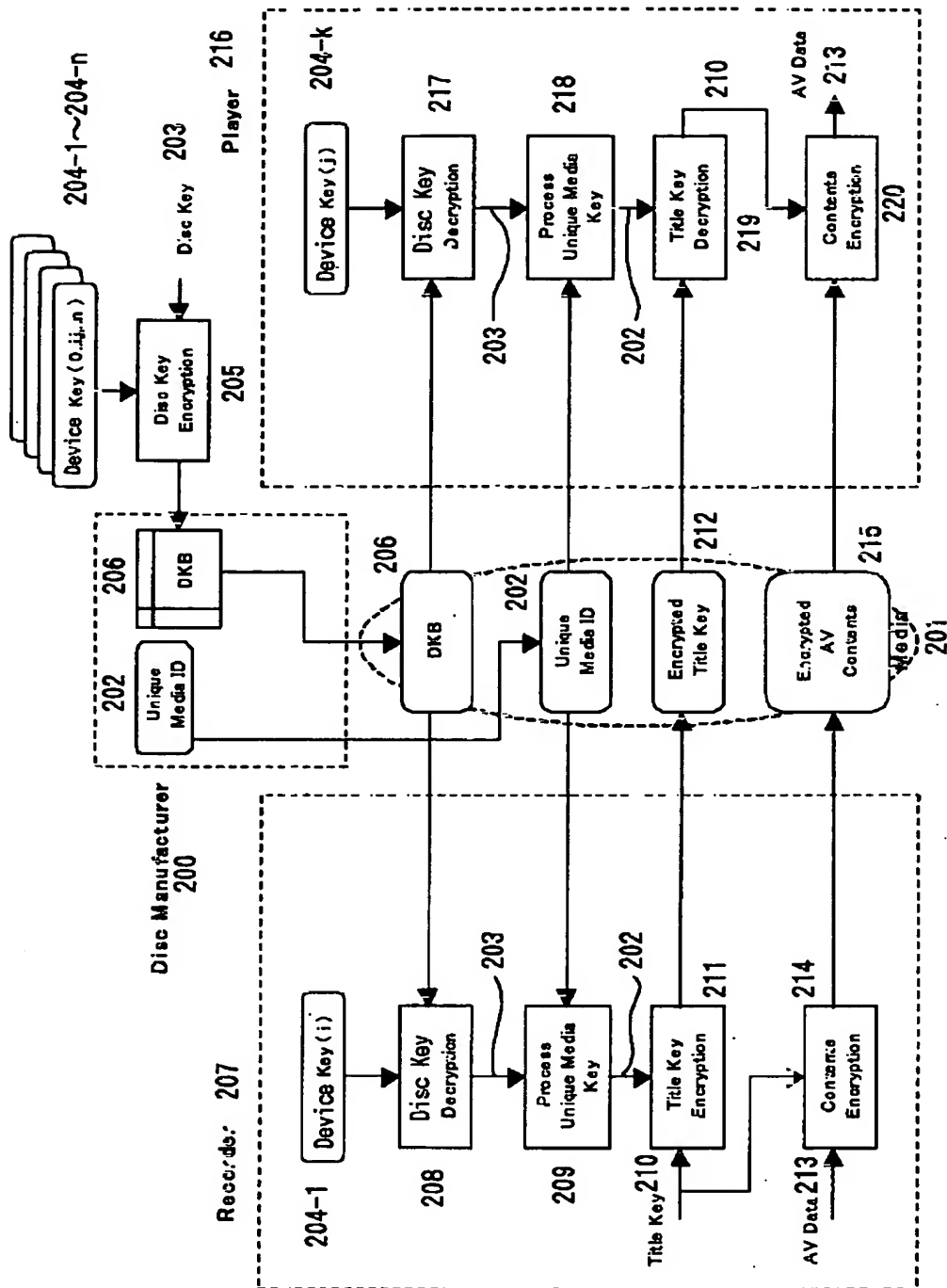
【図8】



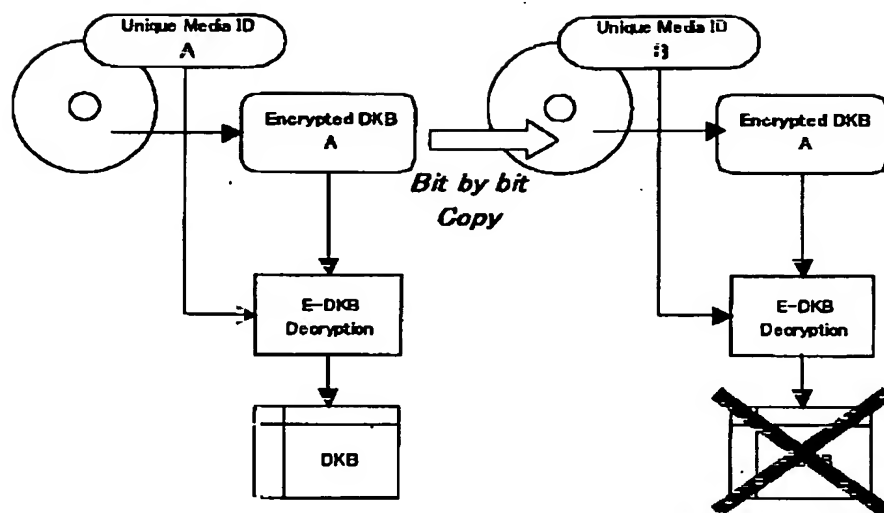
【 図 6 】



【図7】



【 図 9 】



【 図 11 】

初期値 = 「1001」

クロック数	レジスタ値	出力	データステアブル出力
0	1001	1	0
1	1100	0	0
2	0110	0	0
3	1011	1	0
4	1101	1	0
5	1110	0	0
6	0111	1	0
7	0011	1	0
8	0001	1	0
9	0000	0	1
10	1000	0	0
11	0100	0	0
12	1010	0	1
13	0101	1	1
14	0010	0	0
15	1001	1	0
16	1100	0	0
17	0110	0	0
18	1011	1	0
19	1101	1	0
20	1110	0	1
21	0111	1	0
22	0011	1	0
23	0001	1	0

MSd